Lab assignment 2, CS 165

Friday, October 4, 2013

TA: Rachid Ounit, email: rouni001@cs.ucr.edu.

Name: SID: Signature:

The following assignment introduces concepts around congruence, modular arithmetic, coprimality and ends up with the Euler's function.

Part I Congruence

Question 1

Prove all the following properties:

- For a, b, x ∈ ℕ, If x | a and x | b then x | (a+b)
- For a, b, n ∈ ℕ, a*b (mod n) = (a mod n) (b mod n)
- For p ∈ ℕ such that p ≥ 5, if p prime then p ≡1 (mod 6) or p ≡ 5 (mod 6)

I highly recommend you can re-write every proof from class so you can reproduce them in exams.

Question 2

a) Find the solution of the following:

- 29 (mod 3)

- $x \in \mathbb{N}$, $51 \equiv 7 \pmod{x}$
- $x \in \mathbb{N}$, $4x + 2 \equiv 5 \pmod{7}$

b) Solve the following without calculating the initial sum/product/exponent explicitly

- $(243 + 2583) \bmod 3$
- $(248*177*299*492*16) \bmod 7$
- $377^{5} \bmod 11$
- $1056^{27} \bmod 13$

Part II Coprimality

Question 1

Implement a function “gcd” (from the Euclide’s algorithm) for computing the greatest common divisor between two integers. Make sure your program runs efficiently. Then, apply your program on the following cases, and write your results:

gcd(48, 84) = gcd(19, 3214) =

gcd(51, 36) = gcd(353, 215) =

Two numbers a and b are called “coprime” if and only if gcd(a,b) = 1.

Question 2

a) We consider the set Zp = { n, such that $1 \leq n \leq p\text{-}1$ and n coprime with p}. Implement a function φ that takes in argument an integer p and return the number of element in Zp, Apply your program on the following case, and write your results:

φ (3) = φ (7) = φ (19) = φ (21) =

φ (23) = φ (399) = φ(437) = φ (9177) =

b) Use the function *Decompose* (lab 1) for 21, 399, 437 and 9177. Compare φ (21) against φ (3) and φ (7); then φ (399) against φ (3), φ (7), and φ (19); and so on. Do you see any pattern? If so, how would you then improve your implementation of φ?

To go further…

See question on board.